UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/580,952	05/30/2006	Masataka Togashi	288949US2PCT	8918

22850 7590 09/29/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
BRANSKE, HILARY	
ART UNIT	**PAPER NUMBER**
2437	

NOTIFICATION DATE	DELIVERY MODE
09/29/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/580,952	TOGASHI ET AL.	
	Examiner	Art Unit	
	Hilary Branske	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 May 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/30/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to because Item 10 in Fig. 4 refers to "Info Processing Equipment", whereas item 10 in the specification references "GPS Satellite" (page 78, line 24). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character “60” has been used to designate both “NETWORK” in Fig. 9 and "VERIFICATION UNIT" in Fig. 9. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the

application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The disclosure is objected to because of the following informalities:

There is a typographical error on page 21, line 9, where "weather satellite **2**" should be "weather satellite - - 20 - -".

Appropriate correction is required.

Claim 12 is objected to because of the following informalities: There is a typographical error on line 7 of Claim 12, where "certificate authority **serer**" should be "certificate authority - - server - -".

Claim 23 is objected to because of the following informalities: There is a typographical error on line 7 of Claim 23, where "certificate authority **serer**" should be "certificate authority - - server - -".

Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-24 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are directed to software per se, which does not fall into the categories of “process”, “machine”, “manufacture” and “composition of matter”.

Referring to claims 1 and 22, claims 1 and 22 recite the limitations, “information processing equipment”, “certificate issuing server”, and “information storage server”. The specification on page 76, lines 14-20 states that "information processing equipment 30, the certificate issuing server 40, the information storage server 50, and the verification unit 60 each may be configured in part or in full by a computer operable program." This directs the claims to software per se.

Referring to the certificate issuing server of claim 10, claim 10 recites the limitations “a certification request receiving section”, “a certificate issuing section”, and "a certificate transmitting section”. The specification on page 76, lines 14-20 states that "information processing equipment 30, the certificate issuing server 40, the information storage server 50, and the verification unit 60 each may be configured in part or in full by a computer operable program." This directs the claim to software per se.

Referring to the information processing equipment of claims 12 and 23, claims 12 and 23 recite the limitations “information processing section”, “a certification requesting section”, and “an information outputting section”. The specification on page 76, lines 14-20 states that "information processing equipment 30, the certificate issuing server 40,

the information storage server 50, and the verification unit 60 each may be configured in part or in full by a computer operable program." This directs the claims to software per se.

Referring to the information storage server of claims 14 and 24, claims 14 and 24 recite the limitations “information receiving section”, "a storage memory section”, and “a certification outputting section”. The specification on page 76, lines 14-20 states that "information processing equipment 30, the certificate issuing server 40, the information storage server 50, and the verification unit 60 each may be configured in part or in full by a computer operable program." This directs the claims to software per se.

Referring to the verification unit of claim 18, claim 18 recites the limitations "verification receiving section", "a verification memory section", and "a verifying section". The specification on page 76, lines 14-20 states that "information processing equipment 30, the certificate issuing server 40, the information storage server 50, and the verification unit 60 each may be configured in part or in full by a computer operable program." This directs the claim to software per se.

All dependent claims are rejected to as having the same deficiencies as the claims they depend from.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-3, 7-8, 10-14, 16, 19, and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malone et al. (U.S. Patent Application Publication No. US 2004/0125208 A1), hereinafter "Malone", in view of Fischer (U.S. Patent No. 5,659,617), hereinafter "Fischer".

7. **Regarding claim 1,** Malone discloses "certification system," i.e., certification (page 2, section 0023); "comprising: information processing equipment that processes information," i.e., capture device (pages 1-2, section 0018); "a certificate issuing server that issues an electronic certificate to certify the information processing equipment," i.e., the certificate authority issues a Certificate of Authenticity (page 2, section 0023); "and an information storage server that stores information in a storage memory section," i.e., the secure storage facility (pages 2-3, section 0024); "wherein the information processing equipment transmits a certification request to the certificate issuing server," i.e., requesting the certificate (page 4, section 0031); "wherein the certificate issuing server issues the electronic certificate," i.e., the certificate authority generates the certificate (page 4, section 0031); "wherein the information processing equipment receives the electronic certificate issued by the certificate issuing server," i.e., the certificate of authority is sent back to the antenna associated with the capture device (Fig. 1, and page 2, section 0023); "generates certified information based on the electronic certificate and processed information and identification information to identify the certified information," i.e., the capture device stenographically encodes the data with

the certificate and identifying information (page 4, sections 0035-0036, and page 5, sections 0042-0043); "and transmits the certified information and the identification information to the information storage server," i.e., the file is sent to the storage facility (page 2, section 0023); "and wherein the information storage server receives the certified information and the identification information from the information processing equipment and stores the certified information and the identification information in the storage memory section," i.e., the storage facility receives and stores the file with the identifying information (pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "and also receives the identification information, retrieves the certified information stored in the storage memory section, and outputs the certified information retrieved," i.e., the storage facility receives a request for an image and can send the requested image to a remote site (page 3, section 0025).

Malone does not disclose the certificate authority certifying the operating environment of the information processing equipment. Fischer, however, discloses "a certificate issuing server that issues an electronic certificate to certify an operating environment of the information processing equipment," i.e., the location certification unit issues a certificate that authenticates the position of a requestor (col. 2, lines 42-65, and col. 3, lines 40-48); "transmits a certification request of the operating environment of the information processing equipment to the certificate issuing server," i.e., requestor requests a certificate of its position (col. 3, lines 40-48); "wherein the certificate issuing server issues the electronic certificate to certify the operating environment of the information processing equipment based on the certification request of the operating

environment transmitted from the information processing equipment," i.e., the location certification unit provides the certificate of the position to the requestor in response to the request (col. 2, lines 42-65, and col. 3, lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

8. **Regarding claim 2, in view of claim 1,** Fischer discloses "wherein the certificate issuing server certifies time when the information processing equipment operates as the operating environment," i.e. current time (col. 3, lines 40-48).

9. **Regarding claim 3, in view of claim 1,** Fischer discloses "wherein the certificate issuing server certifies location where the information processing equipment operates as the operating environment," i.e., position (col. 2, lines 66-67, col. 3, lines 1-3, and lines 40-48).

10. **Regarding claim 7, in view of claim 1,** Malone discloses "wherein the information processing equipment generates composite information that is made up of the electronic certificate and the processed information," i.e., the certificate is stenographically encoded onto the image and/or audio files (page 4, section 0036); "and transmits the composite information to the information storage server as the certified information," i.e., sends the file to the storage facility (page 2, section 0023); "and wherein the information storage server receives the composite information and the

identification information from the information processing equipment and stores the composite information and the identification information in the storage memory section," i.e., the secure storage facility receives and stores the file and identifying information (pages 2-3, sections 0024-0025, and page 5, section 0043); "and also receives a query including the identification information, retrieves the composite information stored in the storage memory section, and outputs the composite information retrieved," i.e., the storage facility receives a request for an image and can send the requested image to a remote site (page 3, section 0025).

11. **Regarding claim 8, in view of claim 1,** Malone discloses "wherein the information processing equipment generates composite information that is made up of the electronic certificate and the processed information," i.e., the certificate is stenographically encoded onto the image and/or audio files (page 4, section 0036) "calculates a hash value of the composite information," i.e., a hash of the file is calculated (page 5, section 0042); "and transmits the hash value to the information storage server as the certified information," i.e., the hash value is included with the file (page 5, section 0054); "and wherein the information storage server receives the hash value and the identification information from the information processing equipment and stores the hash value and the identification information in the storage memory section," i.e., the storage facility stores the information (pages 2-3, sections 0024-0025) including the hash value and identification (page 5, section 0054); "also receives the composite information, compares the composite information using the hash value, and stores in the storage memory section the composite information compared," i.e., the encrypted

file (page 4, sections 0035-0038) is received by the storage facility and the file is passed through a message digest algorithm to produce a computed hash which is compared to the received hash, and stores the encrypted photograph that has been compared (page 5, sections 0051-0059); "and also receives a query including the identification information, retrieves the composite information stored in the storage memory section, and outputs the composite information retrieved," i.e., the storage facility receives a request for an image and can send the requested image to a remote site (page 3, section 0025).

12. **Regarding claim 10,** Malone discloses "certificate issuing server, which issues an electronic certificate to information processing equipment," i.e., the certificate authority issues a Certificate of Authenticity (page 2, section 0023); "comprising: a certification request receiving section that receives a certification request of the information processing equipment," i.e., the antenna of the certification authority receives the request (page 2, section 0023 and Fig. 1, item 137); "a certificate issuing section that issues an electronic certificate to certify the information processing equipment based on the certification request received by the certification request receiving section," i.e., the certification authority (page 2, section 0023, and Fig. 1, item 135); "and a certificate transmitting section that transmits the electronic certificate issued by the certificate issuing section to the information processing equipment," i.e., the file is transmitted back to the capture device via the antenna (page 2, section 0023, and Fig. 1, item 137).

Malone does not disclose the certificate authority certifying the operating environment of the information processing equipment. Fischer, however, discloses "a certification request receiving section that receives a certification request of an operating environment," i.e., the send / receive unit of the location certificate unit (Fig. 1, item 5, and col. 3, lines 4-14, and lines 40-48); "a certificate issuing section that issues an electronic certificate to certify the operating environment," i.e., the processor of the location certification unit (Fig. 1, item 4, and col. 3, lines 4-14 and lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

13. **Regarding claim 11, in view of claim 10,** Fischer discloses "wherein the certificate issuing server certifies at least one of time when the information processing equipment operates as the operating environment and location where the information processing equipment operates as the operating environment," i.e., current time (col. 3, lines 40-48).

14. **Regarding claim 12,** Malone discloses "Information processing equipment, which processes information," i.e., capture device (pages 1-2, section 0018); "comprising: an information processing section that processes information and stores the information as processed information," i.e., the capture device (Fig. 1, item 102, and pages 1-2, section 0018); "a certification requesting section that transmits a certification

request of the information processing equipment to a certificate authority serer that issues an electronic certificate that certifies the information processing section," i.e., the transmitter transmits requests to the certification authority (Fig. 1, item 134 and page 2, section 0023); "and an information outputting section that receives the electronic certificate issued by the certificate issuing server in reply to the certification request transmitted by the certification request section," i.e., the encryption block receives the certificate which is stored in temporary memory (Fig. 1, item 124); "generates certified information based on the electronic certificate and the processed information as well as identification information to identify the certified information," i.e., encryption is performed on the file including the digital data, certificate, and identification information (page 4, section 0036-0038); "and outputs the certified information and the identification information," i.e., the file and identification information is sent to the storage facility (page 2, section 0023 and page 5, section 0043).

Malone does not disclose requesting certification of an operating environment. Fischer, however, discloses "transmits a certification request of an operating environment," i.e., the requestor transmits a request to certify a reported position (col. 3, lines 4-14, and lines 40-48); "certificate authority server that issues an electronic certificate that certifies the operating environment," i.e., authenticates the position by supplying a certificate (col. 3, lines 4-14 and lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with

Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

15. **Regarding claim 13, in view of claim 12,** Malone discloses "wherein the information processing equipment is a mobile security gadget that acquires information about a security target," i.e., the capture device can be a cell phone or digital camera with forensic, government, or military applications where the security of the information is of great importance (pages 1-2, section 0018, and page 8, sections 0150-0153).

16. **Regarding claim 14,** Malone discloses "information storage server, comprising: an information receiving section that receives from information processing equipment certified information to certify the information processing equipment and identification information to identify the certified information," i.e., the antenna of the storage facility receives the file with the identifying information (Fig. 1, item 140, pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "a storage memory section that stores the certified information and the identification information received by the information receiving section," i.e., the large database stores the file with the identifying information (Fig. 1, item 142, pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "and a certification outputting section that receives a query including the identification information, retrieves the certified information stored in the storage memory section, outputs the certified information retrieved, and thereby certifies the information processing equipment," i.e., the secure storage facility receives a request for the encrypted image and can send the requested image to a remote site (Fig. 1, item 138, and page 3, section 0025).

Malone does not disclose that the certified information certifies an operating environment of the information processing equipment. Fischer, however, discloses "certified information to certify an operating environment," i.e., the certificate certifies a reported position (col. 3, lines 4-14, and lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

17. **Regarding claim 16, in view of claim 1,** Malone discloses "wherein the information processing equipment transmits to the information storage server authentication information to access the information storage server together with the certified information and the identification information," i.e., the storage facility receives from the capture device the file that has been encrypted with the facility's public key (page 2, section 0023, and page 5, sections 0043 and 0051); "and wherein the information storage server receives the certified information, the identification information, and the authentication information from the information processing equipment," i.e., the storage facility receives the information (pages 2-3, sections 0024-0025, and page 5, section 0051); "and stores the certified information and the identification information received in the storage memory section if the authentication information is valid," i.e., if a valid storage facility public key has been used to encrypt

the file, then the outer wrapper can be removed by the storage facility (page 5, section 0052).

18. **Regarding claim 19, in view of claim 12,** Malone discloses "wherein the information processing section photographs an image and stores the image as the processed information," i.e., the capture device captures and stores an image (pages 1-2, sections 0018-0019).

19. **Regarding claim 22,** Malone discloses "a certification system," i.e., certification (page 2, section 0023); "comprising: information processing equipment that processes information," i.e., capture device (pages 1-2, section 0018); "a certificate issuing server that issues an electronic certificate to certify the information processing equipment," i.e., the certificate authority issues a Certificate of Authenticity (page 2, section 0023); "and an information storage server that stores information in a storage memory section," i.e., the secure storage facility (pages 2-3, section 0024); "wherein the information processing equipment transmits a certification request of the information processing equipment to the certificate issuing server," i.e., requesting the certificate (page 4, section 0031); "wherein the certificate issuing server issues the electronic certificate to certify the information processing equipment based on the certification request transmitted from the information processing equipment," i.e., the certificate authority generates the certificate (page 4, section 0031); "wherein the information processing equipment receives the electronic certificate issued by the certificate issuing server," i.e., the certificate of authority is sent back to the antenna associated with the capture device (Fig. 1, and page 2, section 0023); "generates certified information based on the

electronic certificate and processed information," i.e., the capture device stenographically encodes the data with the certificate (page 4, sections 0035-0036, and page 5, sections 0042-0043); "and transmits the certified information to the information storage server," i.e., the file is sent to the storage facility (page 2, section 0023); "and wherein the information storage server receives the certified information from the information processing equipment and stores the certified information in the storage memory section," i.e., the storage facility receives and stores the file with the identifying information (pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "and also receives identification information to identify the certified information, retrieves the certified information stored in the storage memory section based on the identification information received, and outputs the certified information retrieved," i.e., the storage facility receives a request for an image and can send the requested image to a remote site (page 3, section 0025).

Malone does not disclose the certificate authority certifying the operating environment of the information processing equipment. Fischer, however, discloses "a certificate issuing server that issues an electronic certificate to certify an operating environment of the information processing equipment based on the certification request of the operating environment transmitted from the information processing equipment," i.e., the location certification unit issues a certificate that authenticates the position of a requestor (col. 2, lines 42-65, and col. 3, lines 40-48); "transmits a certification request of the operating environment of the information processing equipment to the certificate issuing server," i.e., requestor requests a certificate of its position (col. 3, lines 40-48);

"wherein the certificate issuing server issues the electronic certificate to certify the operating environment of the information processing equipment based on the certification request of the operating environment transmitted from the information processing equipment," i.e., the location certification unit provides the certificate of the position to the requestor in response to the request (col. 2, lines 42-65, and col. 3, lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

20. **Regarding claim 23,** Malone discloses "information processing equipment, which processes information," i.e., capture device (pages 1-2, section 0018); "comprising: an information processing section that processes information and stores the information as processed information," i.e., the capture device (Fig. 1, item 102, and pages 1-2, section 0018); "a certification requesting section that transmits a certification request of the information processing equipment to a certificate authority serer that issues an electronic certificate that certifies the information processing section," i.e., the transmitter transmits requests to the certification authority (Fig. 1, item 134 and page 2, section 0023); "and an information outputting section that receives the electronic certificate issued by the certificate issuing server in reply to the certification request transmitted by the certification requesting section," i.e., the encryption block receives

the certificate which is stored in temporary memory (Fig. 1, item 124); "generates certified information based on the electronic certificate and the processed information," i.e., encryption is performed on the file including the digital data, certificate, and identification information (page 4, section 0036-0038); "and outputs the certified information generated," i.e., the file and identification information is sent to the storage facility (page 2, section 0023 and page 5, section 0043).

Malone does not disclose requesting certification of an operating environment. Fischer, however, discloses "transmits a certification request of an operating environment," i.e., the requestor transmits a request to certify a reported position (col. 3, lines 4-14, and lines 40-48); "certificate authority server that issues an electronic certificate that certifies the operating environment," i.e., authenticates the position by supplying a certificate (col. 3, lines 4-14 and lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

21. **Regarding claim 24,** Malone discloses "information storage server, comprising: an information receiving section that receives certified information to certify the information processing equipment from information processing equipment," i.e., the antenna of the storage facility receives the file with the identifying information (Fig. 1, item 140, pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "a storage

memory section that stores the certified information received by the information receiving section," i.e., the large database stores the file with the identifying information (Fig. 1, item 142, pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "and a certification outputting section that receives a query including identification information to identify the certified information, retrieves the certified information stored in the storage memory section, outputs the certified information retrieved, and thereby certifies the information processing equipment," i.e., the secure storage facility receives a request for the encrypted image and can send the requested image to a remote site (Fig. 1, item 138, and page 3, section 0025).

Malone does not disclose that the certified information certifies an operating environment of the information processing equipment. Fischer, however, discloses "certified information to certify an operating environment," i.e., the certificate certifies a reported position (col. 3, lines 4-14, and lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

22. **Claims 4-6 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malone, in view of Fischer, and further in view of Dube (U.S.**

Patent Application Publication No. US 2002/0199103 A1), hereinafter "Dube".

23. **Regarding claim 4, in view of claim 1,** Malone discloses "wherein the information processing equipment acquires time information indicating a current time, and transmits the time information acquired to the certificate issuing server," i.e., the time is acquired from the GPS information and is included in the file sent to the certification authority (page 2, sections 0021-0023); "wherein the certificate issuing server receives the information from the information processing equipment," i.e., the certificate authority receives a hash of the document (page 4, section 0031).

Malone nor Fischer disclose certifying the specific time associated with the information by attaching unique data. Dube, however, discloses "receives the time information from the information processing equipment," i.e., receives timing signals that include time information (page 5, sections 0047-0048); "attaches unique data available at no other time than a specific time indicated by the time information to the time information," i.e., a random number is calculated based on the fluctuations of received timing signals that is unique to the precise time and location of the receiver (page 5, sections 0049-0051) and stored (page 7, section 0068); "and thereby issues the electronic certificate to certify the specific time," i.e., the certificate is issued and includes the entropy data unique to the specific time (page 7, section 0068, and page 8, sections 0076-0077).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system

that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Dube's technique of generating entropy data based on GPS timing signals received at a specific time in order to reduce the amount of certification processing performed by a local device and increase the security of the generated certificates.

24. **Regarding claim 5, in view of claim 1,** Malone discloses "wherein the information processing equipment acquires location information indicating a location of the information processing equipment, and transmits the location information acquired to the certificate issuing server," i.e., the position is acquired from the GPS information and is included in the file sent to the certification authority (page 2, sections 0021-0023); "and wherein the certificate issuing server receives the location information from the information processing equipment," i.e., the certificate authority receives a hash of the document (page 4, section 0031).

Malone nor Fischer disclose certifying the location associated with the information by attaching unique data. Dube, however, discloses "receives the location information from the information processing equipment," i.e., receives timing signals to pinpoint the current geophysical location (page 5, sections 0047-0048); "attaches unique data available at no other location than a specific location indicated by the location information to the location information," i.e., a random number is calculated based on the fluctuations of received timing signals that is unique to the precise time and location of the receiver (page 5, sections 0049-0051) and stored (page 7, section 0068); "and thereby issues the electronic certificate to certify the specific location," i.e.,

the certificate is issued and includes the entropy data unique to the specific location (page 7, section 0068, and page 8, sections 0076-0077).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Dube's technique of generating entropy data based on GPS timing signals received at a specific location in order to reduce the amount of certification processing performed by a local device and increase the security of the generated certificates.

25. **Regarding claim 6, in view of claim 5,** Malone discloses "certificate issuing server," i.e., certificate authority (Fig. 1, item 135); "issues the electronic certificate," i.e., generates a certificate of authority (page 2, section 0023).

Malone nor Fischer disclose attaching compensation information to the location information. Dube, however, discloses "attaches compensation information to compensate the specific location indicated by the location information to the location information, and thereby issues the electronic certificate," i.e., a normalized timing signal delay is measured to compensate for atmospheric variances (page 5, sections 0049-0051) and the issued certificate includes the delay number (page 7, section 0068, and page 8, sections 0076-0077).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority and

Fischer's technique of remotely certifying location information with Dube's technique of generating compensation data based on GPS timing signals in order to reduce the amount of certification processing performed by a local device and increase the security of the generated certificates.

26. **Regarding claim 21, in view of claim 1,** Malone discloses "certificate issuing server," i.e., certificate authority (Fig. 1, item 135); "certification request," i.e., requesting a certificate (page 2, section 0023); "information processing equipment," i.e., capture device (Fig. 1, item 102); "issues the electronic certificate," i.e., generates a certificate of authority (page 2, section 0023).

Malone does not disclose attaching unique information available only at a current time, or a certification request of an operating environment. Fischer, however, discloses "time information based on the certification request of the operating environment transmitted," i.e., time stamp (col. 3, lines 40-48).

Malone nor Fischer disclose attaching unique information based on the current time. Dube, however, discloses "attaches unique information available at no other time than a current time to time information based on the certification request of the operating environment," i.e., a random number is calculated based on the fluctuations of received timing signals that is unique to the precise time and location of the receiver (page 5, sections 0049-0051) and stored (page 7, section 0068); "and thereby issues the electronic certificate to certify the current time," i.e., the certificate is issued and includes the entropy data unique to the specific time (page 7, section 0068, and page 8, sections 0076-0077).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Dube's technique of generating entropy data based on GPS timing signals received at a specific time in order to reduce the amount of certification processing performed by a local device and increase the security of the generated certificates.

27. **Claims 9, 15, 17, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malone, in view of Fischer, and further in view of Decime (U.S. Patent Application Publication No. US 2004/0039929 A1), hereinafter "Decime".**

28. **Regarding claim 9, in view of claim 1,** Malone discloses a "certificate issuing server," i.e., certificate authority (Fig. 1, item 135); "information storage unit," i.e., storage facility (Fig. 1, item 142).

Malone nor Fischer disclose the certificate issuing server and information storage server are one unit. Decime, however, discloses "wherein the certificate server and the information storage server are one unit," i.e., the certification and validation authority provides a secure repository for evidence and certifies the evidence (Fig. 1, items 118 and 120, page 2, section 0018, and page 4, sections 0047-0049).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system

that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Decime's technique of storing evidence data in a secure repository at the certification and validation authority in order to reduce the amount of certification processing and certified data storage performed by a local device.

29. **Regarding claim 15, in view of claim 14,** Malone nor Fischer disclose storing the order of reception of the certified information received by the information storing section. Decime, however, discloses "wherein the storage memory section further stores an order of reception of the certified information and the identification information received by the information receiving section," i.e., the memory stores metadata relating to received digital content in a manifest, including the time and data in the memory device (Fig. 3, item 320, page 3, sections 0030 and 0038-0039).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Decime's technique of storing evidence data in a secure repository at the certification and validation authority in order to reduce the amount of certification processing and certified data storage performed by a local device.

30. **Regarding claim 17, in view of claim 1,** Malone discloses "a unit that verifies the information processing equipment," i.e., the storage facility receives the encrypted file with the identifying information and ensures that tampering does not occur (Fig. 1,

item 140, pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "wherein the information storage server transmits part of the certified information and part of the identification information stored in the storage memory section to the unit," i.e., the large database stores the file with the identifying information (Fig. 1, item 142, pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "and wherein the unit receives the certified information and the identification information transmitted by the information processing equipment and stores the certified information and the identification information in the memory section," i.e., the files are stored in the database (Fig. 1, item 142, pages 2-3, sections 0024-0025); "and also receives a query including the identification information, retrieves the certified information stored in the memory section, and verifies the information processing equipment with reference to the certified information retrieved," i.e., the secure storage facility receives a request for the encrypted image and can send the requested encrypted image to a remote site, where the encrypted file contains a certificate previously obtained from the certificate authority (page 3, section 0025, and page 4, section 0036).

Malone does not disclose a verification unit or verifying an operating environment of the information processing equipment. Fischer, however, discloses "verifies the operating environment," i.e., the certificate certifies a reported position (col. 3, lines 4-14, and lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with

Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

Neither Malone nor Fischer disclose a verification unit with a verification memory section. Decime, however, discloses "a verification unit equipped with a verification memory section," i.e., the certification and validation authority provides a secure repository for evidence and certifies the evidence (Fig. 1, items 118 and 120, page 2, section 0018, and page 4, sections 0047-0049).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Decime's technique of storing evidence data in a secure repository at the certification and validation authority in order to reduce the amount of certification processing and certified data storage performed by a local device.

31. **Regarding claim 18,** Malone discloses "a unit, comprising: a receiving section that receives certified information and identification information from an information storage server," i.e., the storage facility receives the encrypted file with the identifying information and ensures that tampering does not occur (Fig. 1, item 140, pages 2-3, sections 0024-0025, and page 5, sections 0043-0049); "a memory section that stores the certified information and the identification information received by the receiving section," i.e., the files are stored in the database (Fig. 1, item 142, pages 2-3, sections 0024-0025); "and a section that receives a query including the identification information,

retrieves the certified information stored in the memory section, and verifies information processing equipment with reference to the certified information retrieved," i.e., the secure storage facility receives a request for the encrypted image and can send the requested encrypted image to a remote site, where the encrypted file contains a certificate previously obtained from the certificate authority (page 3, section 0025, and page 4, section 0036).

Malone does not disclose a verification unit or verifying an operating environment of the information processing equipment. Fischer, however, discloses "verifies the operating environment," i.e., the certificate certifies a reported position (col. 3, lines 4-14, and lines 40-48).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority with Fischer's technique of remotely certifying location information in order to reduce the amount of certification processing performed by a local device.

Neither Malone nor Fischer disclose a verification unit with a verification memory section. Decime, however, discloses "a verification unit equipped with a verification memory section," i.e., the certification and validation authority provides a secure repository for evidence and certifies the evidence (Fig. 1, items 118 and 120, page 2, section 0018, and page 4, sections 0047-0049).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system

that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Decime's technique of storing evidence data in a secure repository at the certification and validation authority in order to reduce the amount of certification processing and certified data storage performed by a local device.

32. **Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malone, in view of Fischer, and further in view of Libicki (U.S. Patent No. US 6,237,098 B1), hereinafter "Libicki".**

33. **Regarding claim 20, in view of claim 12,** Malone discloses "information processing section," i.e., capture device (Fig. 1, item 102).

Neither Fischer nor Malone disclose weighing an object and storing a weight. Libicki, however, discloses "weighs an object and stores a weight result as the processed information," i.e., the weight is read and stored in a digital signature (col. 6, lines 12-60).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Malone's forensic communications system that utilizes a local location certification system and a remote certificate authority and Fischer's technique of remotely certifying location information with Libicki's technique of weighing an object and storing the weight in a digital signature in order to reduce the

amount of certification processing performed by a local device and increase the security and versatility of the system by including additional measurements in certificate data.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Skomra et al. (U.S. Patent Application Publication No. US 2005/0076198 A1) disclose providing a digital certificate to a user of an endpoint device by requesting verification of a validation parameter such as location..

MacDoran et al. (U.S. Patent No. 5,757,916) disclose authenticating the identity of a remote user by utilizing location information.

Bell et al. (U.S. Patent Application Publication No. US 2004/0201751 A1) disclose authenticating and signing data from a digital camera using various metadata.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hilary Branske whose telephone number is (571) 270-3395. The examiner can normally be reached on 8:00 a.m. - 6:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Hilary Branske
Examiner, Art Unit 2437

H.B.
Hilary Branske

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437